DETAILED ACTION

1. This is in response to the amendment filed May , , 2008. Claim 1 has been amended. Claims 1-12 are pending and have been considered below.

Claim Objections

2. Claim 1 is objected to because of the following informalities: Line 16 of the claim recites the limitation of “a network server server” . Appropriate correction is required.

3. Claim 2 is objected to because of the following informalities: Line 3 of the claim recites the limitation of “receiving the unique”, the examiner suggests "receiving a unique key' . Appropriate correction is required.

4. in light of the amendment made to claim 1, the previous claim objection has been withdrawn

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 recites the limitation "the software agent" in line 9 there is insufficient antecedent basis for this limitation in the claim.

Claim 1 recites the limitation "the requesting device" in line 20 there is insufficient antecedent basis for this limitation in the claim.

Response to Arguments

6. Applicant's arguments filed 05/06/2008 have been fully considered but they are not persuasive.

7. Applicant has amended the claims, in particular claim 1, to recite that a "user make[s] an initial request for access to the wireless network, the initial request being made from a user-operated device", "the wireless network receive[s] the initial request for access from the user-operated device", and a software agent is installed on the user-operated device, "wherein the software agent is not resident on the user-operated device prior to the initial request for access." Emphasis added.

8. Applicant then argued that "the initial request for data communication starts at the mobile device. In contrast, in Laursen et al, the initial request for data communication starts at the base station." Applicant continued in saying that "Laursen assigns identification information to mobile devices, whereas the present invention receives identification information from mobile devices." See response at page 6 of 8. Emphasis added. The examiner respectfully disagrees because of the following reasons:

9. Contrary to Applicant's assertion, the initial request in Laursen et al starts at the mobile device. For example, at step 702 in Fig. 7A, the fleet managing system receives a fleet data request [0078]. Thus, the initial request must come (start) from the mobile device and not at the base station (or the managing system). See also paragraph [0055]. In paragraph [0057], Laursen et al discloses that the fleet data request is made from a computing device coupled to a landnet 220. In contrast to Applicant's assertion, the initial request for data communication, in Laursen et al, starts at the mobile device as shown above.

10. Applicant also argued that, "both the user(s) and the remote device(s) are authenticated prior to transmission ... In contrast, in Laursen, only the remote device(s) is/are authenticated prior to data transmission. See response at page 6 of 8. Emphasis added.

11. The examiner respectfully disagrees because of the following reasons:

Fig. 3 of Laursen et al shows device info (306) and other info (312) including credential info (314). In addition, Fig. 4 shows device ID (402), subscriber ID (404) and user info (408). Still, Fig. 6 shows user data (606) including username and password. In addition, at step 704 in Fig. 7A, the user "respond[s] with a challenge response" indicative of the user authentication information. See paragraphs [0055], [0056], [0062], [0063] and [0072]. It has been shown as noted above that both the user(s) and the mobile device (s) are authenticated prior to data transmission and that Laursen permits data transfer only after both the user and the device are authenticated.

12. Applicant further argued that Laursen does not te[a]ch (1) transmitting a software agent to a wireless device, and (2) executing the software agent on the wireless device." See response at page 7 of 8. Emphasis added.

13. The examiner respectfully disagrees, in part, because of the following reasons:

It should be noted that by sending a challenge to the mobile device user, the server is in fact downloading a "software agent" to the device since the challenge requires some input from the device. Such "challenge" contains fields/entries that the user has to complete. See paragraphs [0055] and [0056]. As described in paragraph [0057], the user responds to the challenge, which challenge was not resident on the device prior to

the request. More particularly, in paragraph [0072], the user of the mobile device responds with a challenge response prior to authentication. Although not explicitly disclosed in Laursen et al, one of ordinary would know that the challenge response is being provided based on some king of "software agent" being run on the device.

14. Laursen et al does not explicitly disclose, in exact words, transmitting a software agent and executing the software agent, wherein the software agent is not resident on the user- operated device prior to the initial request for access. However, this feature is explicitly described in the patent to Mehring et al (6,609,115). Just like Laursen et al, Mehring et al discloses a method for providing access over a network to a mobile device, wherein a user of the device is required to enter identifying indicia prior to accessing the information. The identifying indicia include device identification and user authentication information (abstract; column 8, lines 24-37). The device comprises of processor for executing a software agent which causes the user information and device identification to be transmitted. See column 2, lines 29-31 and 50-57. More particularly, Mehring et al explicitly discloses that a software agent is automatically installed or downloaded and executed on the user device, wherein the software agent is not resident on the user-operated device prior to the initial request for access. See column 9, lines 34-39, and column 10, lines 57-66).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 1-4, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Mehring et al (US 6,609,115) in further view of Christmas (US 6,085,084) .

Claim 1:Laursen et al discloses a method of automatically providing a secure connection between a wireless network and a user-operated device seeking access to the wireless network (Fig. 2a), the method comprising:

i. Having an individual user make an initial request for access to the wireless network, the initial request being made from a user-operated device(paragraphs [0055], [0057], and [0078]; Fig. 7A, step 702);

ii. Having the wireless network receive the initial request for access from the user-operated device(paragraphs [0 056], [0057]);

iii. Transmitting the device identification and user authentication information to a network server9paragraph [0056]) ; and

iv. Verifying both the device identification and the user authentication information wherein when successfully verified (*At 710, the received credential information is verified by a comparison against corresponding predefined credential information*) (paragraphs [007], [0056]), storing the identification and authentication information on an authorized access list (*the business must be in the list of authorized entities so as to be able to access the fleet managing system*) (paragraph [0054]), providing a unique

encryption key to the device for storage thereon *(Meanwhile commanding mobile station 520 and proxy server 510 exchange encrypt keys and authenticate each other to generate a session key according to a mutually acceptable encryption scheme)(paragraph[0070])* and granting the requesting device access to the wireless network(*otherwise a trust is therefore established between the provisioning entity and the provisioning interface. At 712, the fleet data request from the provisioning entity is granted*)(*paragraph [0079]);* and when unsuccessfully verified (*If there is a disagreement or mismatch between the supplied credential information and predefined credential information, the original request from the provisioning entity is discarded*) (*paragraph [0079]),* storing the identification and authentication information on an unauthorized access list and denying the device access to the wireless network.

However, does not explicitly disclose a step of automatically installing the software agent on the user-operated device, wherein the software agent is not resident on the user-operated device prior to the initial request for access; nor a step of executing the software agent on the user-operated device to gather information from the user-operated requesting device, including device information and user authentication information;

However, Mehring et al discloses a method for limiting online access to restricted documentation, which further discloses:

i. Automatically installing the software agent on the user-operated device, wherein the software agent is not resident on the user-operated device prior to the initial request for access(column 10, lines 57-65);

ii. Executing the software agent on the user-operated device to gather information from the user-operated requesting device, including device information and user authentication information(*column 9, lines 34 -50*);

While neither of them explicitly discloses a step of storing the identification and authentication information on an unauthorized access list.

However, Christmas discloses an automated creation of list of disallowed network points for use in connection blocking which further discloses:

Storing the identification and authentication information on an unauthorized access list (*Fig. 1, item 114*).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Laursen et al and Mehring et al such as to store a list of unauthorized user. One would have been motivated to do so in order to identify unauthorized network access attempts as discloses by Christmas (abstract).

Claim 2: Laursen et al , Mehring et al and Christmas disclose a wireless network as in claim 1 above, and Laursen et al further disclose that the method further comprising, in response to a subsequent request for access to the wireless network by the device (*wherein the provisioning interface receives a request to*

push the fleet data in the memory to the plurality of the mobile stations)

(paragraphs [0016], [0019]) –

i. Receiving the unique key corresponding to the device (*Each of the mobile stations is assigned a device ID 402*) (paragraph [0062], [0066]);

ii. Retrieving the identification and authentication information corresponding to the unique key (*In other words, the user accounts can be kept in a database that is physically placed in any computing device coupled to proxy server 230 and can be collected or fetched therefrom*) (paragraphs [0064], [0066]);

iii. Comparing the identification and authentication information with the authorized and unauthorized lists (*the received credential information is verified by a comparison against corresponding predefined credential information*) (paragraph [0079]); and

v. Based on the comparison, one of granting and denying the device access to the wireless network (*If there is a disagreement or mismatch between the supplied credential information and predefined credential information, the original request from the provisioning entity is discarded otherwise a trust is therefore established between the provisioning entity and the provisioning interface*) (paragraph [0079]).

Claim 3: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, and Mehring et al discloses further discloses that the step of denying access comprises generating a notification message that an

unauthorized device has attempted to access the network (*If the password is not authentic, the addressed web server will send an error message to the remote system*)(column 9, lines 53-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such send a notification message. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

Claim 4: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, and Mehring et al further discloses that the step of granting access comprises providing access in accordance with existing network access rights of the user operating the device (*Based on the criteria and variable data retrieved during the authorization step 168, the policy server 114 determines whether the requesting remote system user has access rights to the requested software application 170*)(column 9, lines 53-67; column 10, lines 1-31). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to provide access based on user access right. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

Claim 8: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, and Mehring et al further discloses that the step of automatically installing application software on the device (*The license server*

144 generates licenses, installs the generated licenses on the remote systems 12 via the network 80, and logs the licenses into the policy/license database 146)(column 12, lines 30-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to automatically install application software. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

Claim 11: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, and Mehring et al further discloses that the step of granting access further comprises conformity to a security policy with respect to access from multiple devices (*Based on the criteria and variable data retrieved during the authorization step 168, the policy server 114 determines whether the requesting remote system user has access rights to the requested software application 170*)(column 9, lines 53-67; column 10, lines 1-31). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to provide access based on user access right. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

17. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Mehring et al(US 6,609,115) and

Christmas (US 6,085,084) as applied to claim 1 above in further view of Weigand (US 7,151,938).

Claim 5: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, while neither of then explicitly discloses that the step of determining the geographical location oft he device. However, Weigand discloses a dynamically managing and reconfiguring wireless mesh network which further discloses a step of collecting information relevant for billing the user for services accessed through the network *(the wireless base station controller may access a geo-location database that correlates billing addresses with positioning information to determine which base station lobes are accessible)*(column 16, lines 38-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al, Mehring et al and Christmas of such to provide information related to billing. The motivation of doing so would have been to limit access to such restricted and highly sensitive data.

Claim 6: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, while neither of then explicitly discloses that the step of collecting information relevant for bandwidth allocation over the network. However, Weigand discloses a dynamically managing and reconfiguring wireless mesh network, which further discloses the step of collecting information relevant for bandwidth allocation over the network (*Reconfiguring the wireless network may include changing bandwidth allocated to a subscriber system participating in*

the lobe pool in the wireless network) (column 16, lines 38-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al, Mehring et al and Christmas of such to provide information related bandwidth. The motivation of doing so would have been to limit access to such restricted and highly sensitive data.

18. Claims 7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Mehring et al(US 6,609,115) and Christmas (US 6,085,084) as applied to claim 1 above in further view of Bade et al (US 6,898,628).

Claim 7: Laursen et al, Mehring et al and Christmas disclose a wireless network as in claim 1 above, while neither of then explicitly discloses that the step of determining the geographical location oft he device. However, Bade et al discloses a method for providing positional authentication, which further discloses that the step of determining the geographical location oft he device (*The system 100 also includes a positioning system 110 that includes at least one transmitter 112, such as a positioning satellite. The positioning system 110 can be any suitable positional access system, such as satellite, microwave, infrared, or radio based, which provides positional access with any suitable method)* (column 3, lines 48-58). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al , Mehring et al and Christmas of such to determine the

geographical location. The motivation of doing so would have been to prevent unauthorized access to the extranet based on locations where access is not allowed on the client machine as disclosed by Bade et al (column 2, lines 16-26).

Claim 10: Laursen et al , Mehring et al and Christmas disclose a wireless network as in claim 1 above, while neither of then explicitly disclose that the network comprises an isolated network segment and the initial connection between the device and the network is limited to the isolated network segment. However, Bade et al discloses a method for providing positional authentication, which further discloses wherein the network comprises an isolated network segment and the initial connection between the device and the network is limited to the isolated network segment (*For instance, an administrator of a host server that contains sensitive and secure data for numerous users located throughout a country, such as the Social Security Office, can restrict access by location with the present invention)* (column 5, lines 26-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al , Mehring et al and Christmas of such to restrict access to the device. The motivation of doing so would have been to prevent unauthorized access to the extranet based on locations where access is not allowed on the client machine as disclosed by Bade et al (column 2, lines 16-26).

19. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Mehring et al(US 6,609,115) and Christmas (US 6,085,084) as applied to claim 1 above in further view of Limsico (US 6,662,228).

Claim 9: Laursen et al , Mehring et al and Christmas disclose a wireless network as in claim 1 above, while neither of then explicitly disclose that wherein the encryption key is a certificate. However, Limsico discloses an internet server authentication client, which further discloses that the encryption key is a certificate (column 4, lines 1-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al, Mehring et al and Christmas of such to provide the certificate as the encryption key. The motivation of doing so would have been to transmit data between machines securely, without possibily of interception or spoofing as disclosed by Limsico (column 1, lines 60-65).

20. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Mehring et al(US 6,609,115) and Christmas (US 6,085,084) as applied to claim 1 above in further view of Bagshaw (US 7,089,426).

Claim 12: Laursen et al , Mehring et al and Christmas disclose a wireless network as in claim 1 above, while neither of then explicitly disclose that the user is defined as a guest user and given a temporary encryption key with guest network access rights. However, Bagshaw discloses a method of encryption, which further discloses wherein the user is defined as a guest user and given a

temporary encryption key with guest network access rights (column 4, lines 21-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al , Mehring et al and Christmas such as to provide a temporary encryption key. The motivation of doing so would have been to limit access to such restricted and highly sensitive data.

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571)

270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Monday, June 16, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136